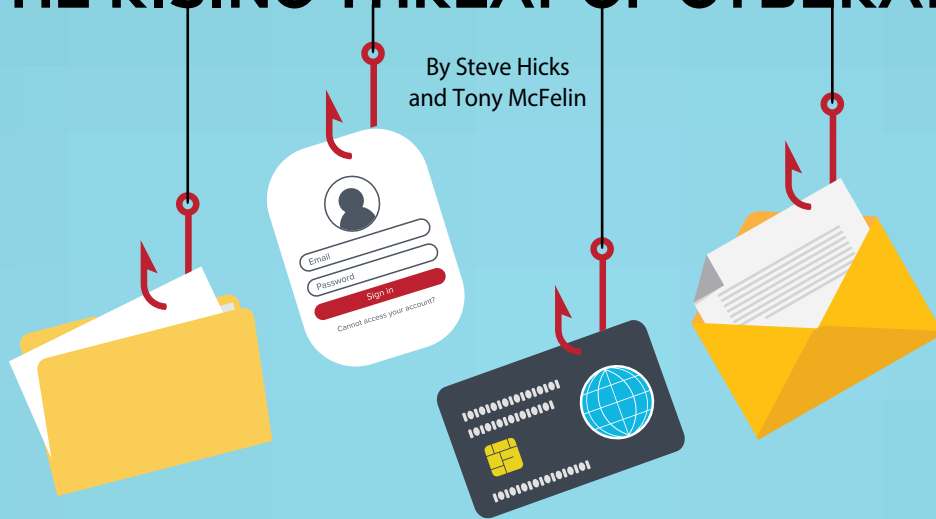


RECOGNIZING RISK:

READYING YOUR BUSINESS FOR THE RISING THREAT OF CYBERATTACKS

By Steve Hicks
and Tony McFelin



By now, business owners in the lumber and building material industry likely understand what a cyberattack is and acknowledge their business could be at risk, but do they understand the extent of damage that can be done and the impact it could have on their business, employees, customers, and even their community?



For a quick glimpse into the level of devastation a cyberattack can cause a business in this industry, one just has to look at the recent experience of a Pennsylvania cabinetry manufacturer. The company was forced to temporarily lay off 500 workers in its small community after a virus took hold of its computer system. Operations were shut down for three weeks, and leadership paid \$250,000 to correct the problem and add additional security measures.

Unfortunately, cyberattacks have ballooned in recent years. According to the Identity Theft Resource Organization, 73% of small business owners said they experienced a data breach or cyberattack in 2023. This figure is up from 43% in 2022 and 58% in 2021. Cyber insurance was reported to be the primary resource for recovery funds by 33% of respondents. Other victims made up for the losses with cash reserves, existing lines of credit, loans, and downsizing measures, among other things.

Cybercrime is a mounting problem impacting any business, and it is not going away. Business owners who understand their risks and take adequate steps to protect their systems from cyberattacks will be best positioned to avoid a costly business interruption and/or hefty financial loss.

TYPES OF CYBER THREATS FACING LUMBER AND BUILDING MATERIAL BUSINESSES

The fact that individuals and business owners are getting better at protecting themselves or their businesses from cyber risks is working against them in a way. With fewer opportunities to hack vulnerable systems, the criminals are now requesting higher ransom payments when they do manage to break in.

While lumber and building material business owners may not see their businesses at high risk because they don't have the data a financial institution does, for example, any business owner runs the risk of endangering sensitive information related to the business, its finances, or merger plans, as well as sensitive information impacting its customers and staff, without proper cyber safety practices in place.

The most common cyber claims we are seeing across the lumber industry involve **misdirected payments**. This type of fraud occurs when money or a product is sent to a fraudulent destination by criminals using fake emails or other forms of communication. Other types of cyber risk facing lumber and building material businesses include:

- **Data Exfiltration:** When cybercriminals hack into a company's system and steal data, requesting a ransom to delete the data.
- **Double Extortion:** A method combining ransomware and extortionware techniques. Instead of the cybercriminals


simply holding data needed for operations for ransom, they threaten to sell it to bad actors over the dark web.

- **Business Email Compromise:** This often involves a vendor whose data system has been compromised. In this situation, the cybercriminal might change the details of the vendor's bank account and send fraudulent invoices, so the payment goes to the thieves.
- **Password Stuffing:** Refers to the criminal act of using breached passwords to gain access to unrelated assets. This can be particularly problematic when individuals use the same password for multiple log-ins.

BEST PRACTICES TO AVOID BECOMING A VICTIM OF A CYBERATTACK

While cybercriminals may be getting more creative to access computer systems and steal valuable data, cybersecurity experts continue to identify new risk mitigation practices. Below is a list of several best practices for lumber and building material business owners and operators to consider:

- Practice good password safety. Do not reuse or share passwords. Consider implementing a password management system.
- Consider layering multi-factor authentication on top of passwords to protect data.
- Conduct quarterly cyber awareness sessions for any staff members who have a company email to help employees stay current on the latest trends in cybercrime and understand how to identify suspicious activity.
- Consider phish testing, which involves leadership simulating a criminal phishing email to track the company's cyber awareness training progress and identify staff members who may need additional training.
- Separate back-office computer systems from operations systems used for equipment, etc., so that human resources, financial, and other sensitive data are not physically in the same location.
- Keep security software updated.

Finally, consult your insurer to better understand your needs and options for cyber coverage. Be sure to ask questions around data compromise response expenses, computer attacks, data compromise liability, network security liability, misdirected payments, and cyber extortion. Understanding your risk and knowing the resources and tactics available to help you prevent losses will help ensure your business is prepared for the future. 

Steve Hicks, AVP – Underwriting, and Tony McFelin, chief information security officer for Pennsylvania Lumbermens Mutual Insurance Company and Managing Consultant, Netrix Global.